Hal S. Shaftel (HS-0627)
Daniel P. Goldberger (DG-2440)
PROSKAUER ROSE LLP
1585 Broadway
New York, New York 10036-8299
Telephone 212.969.3000

Attorneys for Plaintiff Passlogix, Inc.

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PASSLOGIX, INC.,	**Case No. 08 CV 10986 (PKL/MHD)**
Plaintiff,	
against	
2FA TECHNOLOGY, LLC, 2FA, INC., GREGORY SALYARDS and SHAUN CUTTILL,	
Defendants.	

PLAINTIFF PASSLOGIX'S POST-HEARING MEMORANDUM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

In submitting this post-hearing memorandum, plaintiff Passlogix, Inc. ("Passlogix") is respectful and appreciative of the Court's time in addressing the anonymous email sent September 3, 2009 (the "September 3 Email") – which involves serious, disturbing issues that Passlogix only brought to the Court's attention after painstaking investigation.[1]

PRELIMINARY STATEMENT

Both Passlogix and defendants (collectively, "2FA") are in the business of developing and supplying security-related software for managing access to restricted computerized systems. The parties' broader litigation arises from disputes over royalties, deliverables and intellectual property (among other things) under a license agreement. During the discovery period, an unidentified person purporting to work for Passlogix – but providing no substantiation – sent the September 3 Email to (a) two Passlogix senior executives, who just the day before had submitted declarations opposing 2FA's (meritless) motion for a preliminary injunction concerning claimed intellectual property misuse; (b) 2FA principals Gregory Salyards and Shaun Cuttill; and (c) executives at a non-party entity operating in the same security-related software field. [PX 1.] Echoing 2FA's accusations, the email made false but ugly and damaging allegations about Passlogix's claimed "mandate" to "overstep[] the bounds of. . .contractual and ethical obligations" as related to the intellectual property of the other two companies. The email further victimized Passlogix by disclosing confidential technical specifications for a major Passlogix project still under development.

At the start of the hearing, Passlogix asked the Court to "keep its eye" on "two primary and unassailable facts" to be adduced [Tr. 8:6-8]. Both now have been clearly established by

---

[1] As used below, "PX__" refers to Plaintiff's Exhibits at the hearing; "Tr. __" refers to hearing transcript pages; "[Name] Tr. __" refers to deposition transcript excerpts.

compelling evidence: First and foremost, objective, unbiased computer data irrefutably identify the unique computer IP address of Salyards/2FA as the origin of both the September 3 Email and subsequent (repeated) login activity into the account. In the face of that clear proof, Salyards – despite availing himself of extensive discovery into these matters – offers absolutely no competent, credible evidence of any other source. Second, Salyards/2FA admittedly discarded core documentation during the pendency of this case, and such misconduct (a) undercuts their far-fetched theory of some unidentified other person behind the email; and (b) caused Passlogix's investigation to be far more protracted and expensive.

Promptly after receipt of the September 3 Email, 2FA affirmatively raised it with Magistrate Judge Dolinger and exploited the disparaging accusations as pretext to expand discovery and as leverage for settlement. [PX 29, 30, 58.] Passlogix also was forced to address the reputational fallout and related issues with the non-party recipient – which had received Passlogix's highly confidential information that it should not possess. [PX 29.] As an immediate response to the email, Passlogix retained outside counsel to conduct a diligent internal investigation. Only after that (costly) effort found no support for the allegations [PX 34], did Passlogix – having not rushed to judgment – then expand its inquiry externally. It obtained computer records from the internet service, Hushmail.com ("Hush"), through which the September 3 Email was transmitted. Those records tell the unassailable truth: the unique IP address of the sender of the September 3 Email (and the source of subsequent account activity) is registered to Salyards and used regularly by him. [PX 40, 48.] However, Salyards has disclaimed under oath any knowledge about the source of the email.

Confronted now by objective forensic proof about the September 3 Email, Salyards resorts to arguing that some unknown person, for some inexplicable reason, copied or "spoofed" his IP address. That theory is simply not sustainable: the unrebutted expert testimony from

Andrew P. Obuchowski, a long-time law enforcement official with computer forensic expertise, is clear that the data captured on the Hush logs was not – and could not be – spoofed. [Tr. 147:15-21.] Even if technologically feasible (which it is not), there is no evidence of anyone having spoofed the IP address. Based on nothing but unreliable – inadmissible – suspicion, Salyards speculates that a now-former Passlogix employee (Joe Robinson) may have sent the email. But the September 3 Email is flatly inconsistent with undeniable facts about Robinson and his work experience. Indeed, Salyards' own proclaimed linguistic expert stated the view that Robinson, based upon a review of Robinson's writings, was not the author. [Tr. 308:2-6.]

As part of its investigation into the September 3 Email, Passlogix also considered an earlier anonymous email transmitted though the Hush website on April 13, 2009 (the "April 13 Email") [PX 2] – the only other anonymous, Hush email that Passlogix management has ever received. The text of the April 13 Email is notable in two respects: (a) it disparages a Passlogix employee in regard to dealings with several non-parties, and it surfaced within days of a dispute over 2FA's tactic (ultimately precluded by Magistrate Judge Dolinger) to subpoena these very same entities; and (b) it raises the specter of Passlogix's "legal issues . . . spill[ing] over to this account." And sure enough, the computer logs from Hush identify IP addresses associated with Salyards as the origin of the April 13 Email and subsequent logins into that account – IP addresses not only for Salyards' office and residence, but also to a San Francisco hotel at which he stayed during part of the period that the Hush account was accessed. [PX 38, 49.]

Although Salyards relies heavily on deposition testimony from a disgruntled former Passlogix employee (Chris Collier) who claims to have sent the April 13 Email from 2FA's offices and later "spoofed" Salyards' IP address, that testimony does not withstand scrutiny: in fact, it does not even provide support to Salyards for the critical September 3 Email, which Collier states he did not send and does not know who did. [Collier Tr. 65:11-17.] Even with

respect to the April 13 Email, (a) the unrebutted expert testimony from Obuchowski refutes Collier's claims about the ability to spoof an IP address; (b) Collier testified incorrectly about basic facts concerning the Hush account; (c) no computer logs or other data corroborate Collier's transmittal of the email (and in fact are inconsistent with it); and (d) Collier lacks credibility: among other things, he interacted extensively with Salyards/2FA – even while employed by Passlogix – unbeknownst to Passlogix and contrary to its interests; plus, he has reversed his statements about the emails and now claims that he was previously untruthful.

The compelling computer data and other evidence tying Salyards to the September 3 Email (and April 13 Email) is only half of the story. As Salyards has sought to dodge the hard facts, he has been forced to admit to discarding the very records that his own self-serving assertions put at issue. This is particularly troublesome, since Passlogix has been entirely forthcoming in disclosing information about the emails: it even waived the attorney-client privilege as related to its confidential internal investigation, producing not only the report but also the underlying notes and drafts. [PX 34-35.] In stark contrast, what has come to light is that Salyards/2FA spoliated underlying records that could further confirm his culpability and stymied disclosure of relevant information: Salyards admits to destroying during the pendency of this case (and then keeping it secret from Passlogix for months) another claimed anonymous email from a Hush account that allegedly also attached Passlogix confidential technical specifications similar to the September 3 Email. He admits discarding during this case all of his over 150 written communications with Collier, on whom he places all weight for the April 13 Email. By improperly invoking the attorney-client privilege, 2FA also blocked deposition questions asked of Cuttill in order to conceal communications with Collier and later ambush Passlogix at the neatly choreographed Collier deposition.

As summarized below in greater detail, the evidence is clear and convincing – indeed, overwhelming – that Salyards was the source of the September 3 Email (and the April 13 Email). When found out, Salyards sought to cover his tracks, and he destroyed the very records implicated by his contention that some other person(s) used his IP addresses in disguise. That destruction of records not only belies Salyards' self-serving assertions, but also made it far more difficult, time-consuming and expensive for Passlogix to compile the comprehensive facts about the provenance of the emails. Although Passlogix is sensitive to the gravity of these issues and the high standard of proof applicable here, it respectfully submits that the compelling evidence justifies severe sanctions: Salyards/2FA's pleadings should be dismissed, and Salyards should reimburse Passlogix for the costs that Passlogix incurred in addressing these emails.

I. COMPELLING EVIDENCE REFUTES SALYARDS' DENIAL OF SENDING THE SEPTEMBER 3 EMAIL

A. Circumstances Surrounding the September 3 Email:

In what Passlogix views – and so argued to the Court – to be a stunt, 2FA brought a motion for preliminary injunction, in August 2009, on the theory that Passlogix misappropriated trade secrets and/or intellectual property. On the very day after Passlogix filed its opposition, Passlogix received the anonymous September 3 Email. [PX 1.] The email was sent to Passlogix's President & CEO (Marc Boroditsky) and Chief Technology Officer (Marc Manza) – the very two persons who submitted declarations the day before. The email also was copied to 2FA's principals, as well as to two executives at a non-party business named Imprivata (which had acquired assets from a bankrupt entity from which a team of engineers transitioned to Passlogix). In striking similarity to 2FA's preliminary injunction accusations, the email alleged that Passlogix had a "recent mandate to utilise Imprivata and 2FA information that clearly oversteps . . . contractual and ethical obligations." The author purports to "have transitioned earlier this year" to Passlogix and is "appalled by the unprofessionalism and unethical behavior".

The email also attached a copy of Passlogix's confidential technical specifications for a major project still under development. That dissemination created a serious risk of competitive harm and lost investment for Passlogix, particularly given the nature of Imprivata's own business. [Tr. 23:24-24:3; 24:15-20; 503:10-22.][2]

2FA immediately jumped to exploit the September 3 Email: by about noon the very next day, 2FA's counsel wrote Passlogix's counsel that "my client takes the allegations set forth in the email very seriously" and demanded production of various documents including "all documents related" to the referenced non-public project. [PX 58.] Soon thereafter, Salyards himself wrote Boroditsky, urging him to accept 2FA's latest settlement proposal, and informed him that "[o]ur attorney plans on raising the issue with the court this week." [PX 29.] Next, on September 14, 2FA's lawyer sent a letter to the Magistrate Judge "to bring to [the Court's] attention an anonymous email received by 2FA", and "notice[d] its intent to file a Motion to Compel" all documents concerning Passlogix's non-public project – which it later did (but which ultimately was denied). [PX 30.]

By these communications (including the correspondence to the Magistrate Judge), 2FA affirmatively used the September 3 Email as negotiating leverage before the settlement conferences on September 16 and October 1, 2009. Even more significantly, 2FA interjected the email into the case as pretext for demanding broad document and deposition discovery into Passlogix's operations – as it itself stated by letter to the Magistrate Judge on September 14. [PX 30.] In particular, 2FA made repeated demands to expand disclosure into the confidential project

[2] Taking a prudent approach, Boroditsky wrote as follows to both 2FA and Imprivata within hours of receiving the September 3 Email [PX 29]: "Passlogix's management is aware of no basis for the anonymous allegations", but "intend[s] to thoroughly inquire further into this serious matter." In light of the disclosure of Passlogix confidential information, Boroditsky further wrote: "the email unlawfully transmitted Passlogix confidential and proprietary intellectual property" and "[y]ou are instructed not to review or further transmit the information."

described in the technical specifications attached to the email, and for other discovery concerning the experience and conduct of the personnel involved in developing the project. Although 2FA was largely (but by no means entirely) rebuffed by the Magistrate Judge in its efforts on these fronts, the fact remains it persistently sought to take advantage of the email.[3]

B. Passlogix Thoroughly Investigated the September 3 Email

Despite no indicia of validity to the September 3 Email, Passlogix acted responsibly and retained outside counsel to investigate the matter thoroughly – at substantial burden and expense. Passlogix undertook the effort because it wanted to be prudent and proactive about its internal affairs. Passlogix also, however, had to address 2FA's opportunistic use of the email. There also was the need to handle the situation with Imprivata, which had brought its own counsel into discussions both about the allegations of the email and the handling of the confidential Passlogix information impermissibly sent to Imprivata. [Tr. 503:10-22.]

At no time did Passlogix rush to blame any outside source for the September 3 Email. Only after the independent inquiry – encompassing over 25 employee interviews – found no source for the allegations [PX 34; Tr. 35:8-36:3, 16-22], did Passlogix then turn to investigate externally. The interview process alone cost Passlogix in excess of $50,000 in outside counsel fees, not to mention the internal costs and disruptions, and the additional legal costs dealing with both 2FA and Imprivata on these matters. [Tr. 38:22-24; 85:14-17; 87:3-6.]

Passlogix next served a subpoena on the Hush website, in Canada, for the computer logs showing the originating IP addresses associated with all the account activity. Hush produced an internet activity log (the "September 3 Hush Log"), which displays the IP address and date and

---

[3] On multiple occasions, the Magistrate Judge found that 2FA improperly sought unjustified discovery into the specifics of the project under development. See 11/25 Tr. 5:17-11:2; 12/21 Order, Docket No. 47; Womacks Tr. 37:24-43:30.

time for each action taken in connection with the September 3 Email account. [PX 48; Tr. 154:5-6.][4] The originating IP address is the IP address of the source computer or network from which the connection to Hush was established. [Tr. 154:1-6.] The September 3 Hush Log reflects the originating IP address for the creation of the account on September 3, 2009 at 2:10 PM CDT [App. A, No. 1] (at 2:00 PM CDT, it is known Salyards was in his office [Tr. 434:2-9]); the sending of the September 3 Email itself at 4:00 PM CDT [App. A, No. 12]; and the other account activity on September 3 and 4. [PX 48; App. A, Nos. 6, 10, 24, 28.] For each login or transmittal relating to the September 3 Email account, Hush captured the originating IP address of 70.114.246.62.

Using pubic directories, Passlogix next traced the IP address 70.114.246.62 to Cedar Park, Texas, where it was assigned by the internet service provider ("ISP") Time Warner. Knowing from its business dealings that Salyards and 2FA's offices are located in Texas, Passlogix compared the IP address identified by Hush with the IP addresses of multiple prior emails received from Salyards. It was discovered that they matched. [Tr. 40:9-41:5.] Passlogix thereafter served a subpoena on Time Warner to further confirm that the IP address from the Hush log corresponds to Salyards' IP address. Records obtained from Time Warner show that the IP address used for the September 3 Email account is registered to Salyards at 2FA's business address ("Salyards' Business IP"). [Tr. 156:6-20; PX 40.] The IP address captured by the September 3 Hush Log for each action taken in connection with the account is Salyards'

---

[4] The principal data from the Hush computer logs was accepted into evidence as PX 48 and PX 49. To convert the time details from the logs (which are stated in "UTC" time, another name for "Greenwich Mean Time") to the time corresponding to Salyards' location (either "CDT" or "PDT" depending on the particular day), an annotated version of the computer log exhibits are annexed hereto as Appendices ("App.") "A" and "B" respectively.

Business IP. Passlogix also retained Obuchowski to provide expert assistance in analyzing the Hush records and related email data.[5]

C. Compelling Evidence Demonstrates That Salyards Is The Author

At his deposition (and again at the hearing), Salyards repeatedly denied under oath any involvement in, or knowledge of, the transmittal of the September 3 Email (and April 13 Email). [Tr. 383:8-384:4; 385:3-4, 11-13; 395:8-19.] However, the basic computer records from Hush, as matched against Time Warner records and Salyards' own emails, show that the September 3 Email was sent from an IP address registered to Salyards and that the account was subsequently (and repeatedly) accessed from that same IP address. As Passlogix's computer forensic expert, Obuchowski, testified without contradiction, the Hush records reliably record the actual originating IP address, so here is no reason to doubt the authenticity or accuracy of the Hush records. [Tr. 187:3-12; 229:20-21; 230:7-11, 19-24; 615:8-16.] Simply put, there is no evidence linking anyone but Salyards to the September 3 Email.

1. No "IP Spoofing" Occurred:

Without any support, Salyards argues that his Business IP appears on the September 3 Hush Log because it was "spoofed" by some unidentified person, for some unknown reason. [DX 2: 2FA Letter, dated October 29, 2009 at 1-2.] IP spoofing is a term used to describe the process of concealing in limited circumstances one's IP address to make a computer communication appear to come from a different source. [Tr. 147:4-10.] However, as Obuchowski testified, the type of IP spoofing alleged by defendants – which involves changing Salyards' public IP address assigned by his ISP Time Warner – could not occur here because it is

[5] Obuchowski spent 12 years in law enforcement where, as a member of a computer crime task force, he conducted numerous computer crime investigations. He has also taught computer forensics at police academies and at colleges, and has been previously qualified as an expert in federal court, where he testified about IP spoofing. [PX 36 at ¶ 1, Ex. 1; Tr. 145:11-146:18.]

not possible to spoof this type of IP address when connecting to an internet website like Hush. [Tr. 147:15-21.] This is true for several reasons:

First, in unrebutted expert testimony, Obuchowski stated that there is no software on the market that can be used to spoof a public IP address assigned by an ISP like Time Warner, such as Salyards' Business IP. [Tr. 164:6-19; 242:12-16; 623:17-624:2.]

Second, in order to access a website on the internet, two computers (or networks) must be able to communicate with each other. They do so by sending information back and forth to each other's IP address (the same way a telephone number corresponds to a telephone, an IP address corresponds to a computer and/or network). [Tr. 146:19-147:3.] Here, if someone tried to access the Hush website and conceal their own IP address by "spoofing" another IP address, then Hush would respond back by sending information to the computer/network associated with the "spoofed" IP address, not to the concealed IP address. As a result, the spoofer would never be able to complete the process of logging into the Hush website or complete any other activity, because he/she would not receive communication back from the Hush website as it would instead be directed to the spoofed IP address. [Tr. 615:8-16.]

Third, email header records[6] from the September 3 Email further confirm that no spoofing took place. Obuchowski forensically examined the email header records from the September 3 Email and found no indicia of spoofing. [PX 36 at ¶ 3-15; Tr. 170:15-18.] If – as defendants contend – the September 3 Email had been sent from a location other than 2FA, by someone other than Salyards, then there would have been indicia of spoofing contained in the email internet headers, including inconsistencies in the header data. [PX 36 at ¶ 15.] However, Obuchowski found no such irregularities, nor any indicia of spoofing. [Tr. 168:21-169:16;

[6] Email headers consist of technical information embedded within the e-mail that shows properties relating to its transmission. [Tr. 170:11-14.]

616:20-617:4; PX 36 at ¶ 14-15.] Based upon an examination of all the evidence – consisting of the September 3 Hush Log, the email header records, and other relevant internet records – Obuchowski concluded that the email was sent from Salyards' Business IP and that that no spoofing could even have occurred. [Tr. 153:6-16; 616:20-617:4; PX 36 at ¶ 14-15.]

2. No Evidence of Any other Author of the September 3 Email:

Not only do the Hush logs provide clear, concrete evidence of Salyards' transmittal of the September 3 Email (and repeated login activity thereafter in relation to the account), but no evidence exists of any other author. That is so, even though Salyards obtained expansive discovery from Passlogix concerning the September 3 Email, including (among other things) depositions of nine current and former Passlogix employees to whom questions about the email allegations were asked; personnel records of individuals who Salyards identified as relevant to the email; and comprehensive documents concerning Passlogix's internal investigation (for which Passlogix agreed to waive the attorney-client privilege). Despite all that discovery, Salyards relies only on the entirely unsubstantiated "suspicion" of Chris Collier [Collier Tr. 65:11-66:2], a former Passlogix employee, that another former employee, Joe Robinson, might have sent the email. See Rylott-Rooney v. Alitalia-Linee Aeree Italiane SpA, No. 07 Civ. 11091, 2009 WL 37817, at *2 (S.D.N.Y. Jan. 6, 2009) ("opinion [testimony], based on speculation, is inadmissible"); Washington v. Dep't. of Transp., 8 F.3d 296, 300 (5th Cir. 1993) ("speculative opinion testimony by lay witnesses . . . is generally considered inadmissible"). It is notable that 2FA's own proffered linguistic expert testified that, based on his review of requested Robinson writings, Robinson did not appear to be the author. [Tr. 308:2-6.]

The last time Collier had communicated with Robinson was at least several months before September 3 [Collier Tr. 77:17-78:12] – and he thus has no foundation to opine. Even apart from the inadmissibility of Collier's claimed suspicion, as well as Collier's own credibility

gap, Robinson factually does not fit the profile of the author: not only did he disavow any knowledge during the internal investigation [PX 34], but the evidence shows he generally was positive about his Passlogix experience. [DX 12 at PL0096104.] Contrary to the September 3 Email author's statements, Robinson did not receive a "monthly paycheck", but a bi-weekly one [Tr. 47:24-48:6]; did not "stop assisting on the SAW project" in the September 3 timeframe, but rather had just returned from an excused absence and worked throughout the month of September on the SAW project [Tr. 48:12-15; 127:7-19; 129:1-10; Womacks Tr. 25:16-26:24; 30:20-32:7]; had not interacted for several months with Marc Manza to "have been treated like a second-class citizen by" him [Tr. 123:25-124:5]; and did not have "more than 15 years of development experience" [Tr. 48:7-11; 93:17-20.] Nor did Robinson or anyone else thereafter "share" any "additional information" with 2FA as the author proposed. [Tr. 468:8-469:5.]

3. Salyards Misplaces Reliance on Linguistic Analysis:

Salyards presented evidence from a purported linguistic "expert", Prof. Alan Perlman, who the Court did not qualify. Instead, the Court stated it would hear the testimony and then weigh whether to credit it at all. [Tr. 260:25-261:4.] Perlman never has been qualified by any court, never has published any scholarship on the issue of identifying anonymous authorship, and last held an academic position 31 years ago. [Tr. 247:6-15; 253:16-19.] Aside from the lack of proper credentials, the methodology Perlman used to try to exclude Salyards as author of the September 3 Email is nothing short of junk science. Although Perlman testified that "more data" is always preferable [Tr. 272:25-273:6], all he did was review roughly 60 emails that 2FA self-selected for him – out of many hundreds of possible emails and other writings. He had no idea what criteria was used to select the small subset he received and he applied no statistical analysis to determine its representativeness or significance. [Tr. 255:7-12; 274:6.] Nor did he make any

inquiry to check if key phrases in the September 3 Email appear in any of Salyards' numerous other emails that were not provided to him by 2FA. [Tr. 273:14-274:24.]

Thus, when Perlman testified that certain phrases or styles did not appear in Salyards' writings, he admitted on cross-examination that all he meant is that they did not appear in the small, unrepresentative subset of 60 emails he reviewed – he certainly could not state that they did not appear in other of Salyards' extensive writings. To the contrary, Perlman was shown multiple examples where, in fact, the very phrases he focused on, were elsewhere used by Salyards. For instance, Perlman testified that a critical, distinctive characteristic of the September 3 Email is the presence of sentences beginning with he word "Having. . .". He claimed that the sample of Salyards' writings he reviewed did not reflect that distinctive characteristic. [Tr. 296:22-300:9.] However, there are multiple instances in other writings where Salyards begins sentences with the word "Having . . ." – the very tell-tale sign that Perlman himself emphasized to evaluate authorship. [PX 6 at PL0042567, PX 7 at PL0042562, PX 16 at PL0031594.]

4. Salyards Misplaces Reliance on Friendly Restaurant Witnesses:

Salyards alleges that three friends and his wife were with him at the Pluckers restaurant near Austin (the "Restaurant Witnesses") at 4:00 PM CDT on September 3, when the email was sent. But the claimed recollections from these friendly witnesses (Troy Dunson, Kendall Posey, Benjamin Dismore and Annalisa Salyards) – each of whom arrived and left at different times – are inconsistent and contradictory. They submitted declarations 48 days after the September 3 gathering (except for Mrs. Salyards, who provided no declaration), and were deposed nearly three months after September 3 (on December 2) – thus, the precision of the testimony is inherently suspect. Given the context here – where the timing details matter – the witnesses admit that their recollections are estimates at best: "Keep in mind that, you know, over a month

had passed [before signing the declaration], a month and half had passed, so, you know . . . I don't remember the exact times" [Dismore Tr. 7:14-19]; "I didn't really remember too, too much. I mean it was a long time ago." [Dunson Tr. 9:20-21.] To further compound the lack of reliability, two witnesses – Posey and Dunson – each consumed at least three pints of beer while at the restaurant. [Posey Tr. 12:9-14; Dunson Tr. 16:21-17:3.]

Most importantly, the Restaurant Witnesses' own accounts of when Salyards arrived at the restaurant differ from one another and also from Salyards' own account. Dismore could not "remember exact times" but believes Salyards arrived "probably around 4:00 or 5:00" [Dismore Tr. 7:19; 10:8-10] – which would place Salyards' arrival after the email was sent. While Salyards claims that he left his office for the restaurant at "like 3:30 or so" and arrived by 4:00 [Tr. 434:2-9], Posey recalled Salyards arriving at "approximately 3:15" [Posey Tr. 16:15-17]; Dunson recalled Salyards arriving at "3:15, 3:30-ish" [Dunson Tr. 14:10-12]; and all Salyards' wife could recall was that she arrived sometime that afternoon, and believes that Salyards was already there. [A. Salyards Tr. 6:9-21.]

The Restaurant Witness recollections are similarly inconsistent regarding the timing they themselves arrived at the restaurant. For example, Dismore recalled that he and Dunson arrived together around noon or 1:00 PM and that his girlfriend met them there around 5:00 PM. [Dismore Tr. 8:20-9:2, 9:5-6.] Dunson, however, recalled arriving alone – between 2:00 and 2:30 – and that that Dismore and his girlfriend were already at the restaurant when he arrived. [Dunson Tr. 13:5-6, 20-25.] Furthermore, accounts differ as to whether Salyards arrived with his wife and children or before his wife and children, and even as to who was present at the restaurant that evening. Nor could any remember what Salyards was wearing. [A. Salyards Tr. 8:6-8; Posey Tr. 13:18-20; Dunson Tr. 17:24-18:1.]

Moreover, other aspects of Salyards' account are not corroborated by any of the Restaurant Witnesses. Salyards testified that after leaving the restaurant around 4:45 with his family, he went back to the office and then returned to the restaurant from 6:00-7:00 PM while "[e]verybody was closing out." [Tr. 435:2-18.] He also testified that he picked up the cash he had left with his friends and paid with a credit card. [Tr. 435:16-17.] However, not one of the Restaurant Witnesses testified about Salyards returning. For example, Posey merely testified that Salyards left "before the rest of the group so he left cash for the table" [Posey Tr. 14:3-7.][7]

Due to the inconsistencies and contradictions among the Restaurant Witnesses themselves and with Salyards' own account, this testimony does not come close to substantiating Salyards' whereabouts at the precise time the September 3 Email was sent.

II. COMPELLING EVIDENCE REFUTES SALYARDS' DENIAL OF SENDING THE APRIL 13 EMAIL

Similar to the September 3 Email, computer records and other evidence conclusively tie Salyards to the only other anonymous email sent to Passlogix management through the Hush internet service – the April 13 Email. The basic point is to reveal a pattern of misconduct, and thereby corroborate Salyards' culpability for the critical September 3 Email. Even independent of the April 13 Email, however, the facts specific to the September 3 Email stand on their own in showing that Salyards sent it.

A. Circumstances Surrounding the April 13 Email:

On April 9, 2009, 2FA wrote a letter announcing its intention to serve subpoenas on certain Passlogix customers. [PX 22.] Among the entities listed were Wal-Mart, Deloitte and

---

[7] At the conference held on November 9, 2009, the Court directed Salyards to produce receipts from the September 3 gathering at the restaurant. [11/9 Tr. 50:6-13.] However, Salyards failed to produce responsive receipts from any of the Restaurant Witnesses or himself.

Touche and Oracle. On April 13, Passlogix wrote to the Court vigorously opposing the subpoenas because the entities listed were not relevant to the case and instead were a tactic for harassment.[8] On the very same day, Passlogix's CEO Marc Boroditsky and Vice President-Sales Mark Gillespie received the anonymous April 13 Email – which makes reference to each of the three above-identified entities.

The substance of the April 13 Email primarily relates to Passlogix customer Wal-Mart – with whom Passlogix was then in the process of finalizing an agreement, but also makes reference to Oracle, as well as an executive, Adnan, from Deloitte and Touche (all companies that 2FA was seeking to subpoena). [PX 2.] The author claims that Passlogix is in jeopardy of losing the Wal-Mart account because a certain Passlogix executive was leaking Passlogix's information. In addition, the email references 2FA and gratuitously claims that the Deloitte and Touche executive "has a lot of respect for [Salyards]." The author warns Boroditsky that "[h]opefully, Passlogix's legal issues will not spill over to this account."

At the time it was received, the April 13 Email did not appear to require any urgent reaction. Boroditsky responded to the anonymous author: "It's hard to take anonymous information seriously. . . If you can support your claim with facts there is no need to hide." [PX 26.] It was only after September 3, when the later Hush email became the subject of intensive scrutiny, did Passlogix recognize that the prior Hush email from April may bear some relation to the later email. As part of its investigation into the September 3 Email, Passlogxing thus subpoenaed records from Hush concerning the account associated with the April 13 Email.

---

[8] In fact, the Magistrate Judge rejected 2FA's application as merely being "tit for tat" tactics. [4/23 Tr. 12:7-17.]

At his deposition (and again at the hearing), Salyards denied any involvement in, or knowledge of, the transmittal of the April 13 Email. [Tr. 371:14-21; 383:21-384:4; 384:25-385:2, 5-19.]

B. Compelling Evidence Demonstrates That Salyards Is The Author:

1. Detailed Internet Logs Track Salyards' Movements:

The log received from Hush for the account involved in the April 13 Email (the "April 13 Hush Log") captures three separate IP addresses, all of which are associated with Salyards:

- 70.114.246.62 (Salyards' Business IP): this IP address, as explained above, is assigned by Time Warner and registered to Salyards, at 2FA's business address. [PX 40.]
- 70.114.204.202 ("Salyards' Home IP"): this IP address is assigned by Time Warner and registered to Salyards' wife, at Salyards' home address. [PX 40.]
- 64.186.161.2 (the "Mark Hopkins IP"): this IP address is registered to the Mark Hopkins Hotel in San Francisco. The April 13 Hush Log captured this IP address twice – on April 20 and April 23, 2009 – while Salyards was staying at the Mark Hopkins Hotel for a conference. [PX 38.]

No evidence calls into question the accuracy of the April 13 Hush Log. While the September 3 Hush Log reflects Salyards' Business IP Address, the April 13 Hush Log reflects IP addresses that notably shift from Salyards' office to his home in Austin; from Austin to a specific San Francisco hotel, where he stayed while attending a conference; and then back to Austin. For example, within a 23-hour period – from April 13 at 6:15 PM CDT to April 14 at 3:19 PM CDT – the IP address captured by Hush changes from Salyards' Business IP (at 6:15 PM CDT on April 13) [App. B, No. 23] to Salyards' Home IP (at 10:38 PM CDT on April 13) [App. B, No. 24] and then back to the Business IP (at 3:19 PM CDT on April 14) [App. B, No. 30]. [PX 49.]

It is nonsensical that someone "spoofing" Salyards would have used multiple different IP addresses in such a very short timeframe.

The April 13 Hush Log reflects that the account was accessed twice from the Mark Hopkins Hotel in San Francisco – once on April 20 at 10:30 AM PDT [App. B, No. 46], and once on April 23 at 10:15 PM CDT [App. B, No. 50]. [PX 49.] Records obtained from the Mark Hopkins confirm that Salyards was a guest at the hotel between April 19, 2009 and April 24, 2009. [PX 36.] It is compelling that the only two instances that the account was accessed from the Mark Hopkins occurred while Salyards was a guest there. The records also confirm that Salyards purchased internet access, which was active during both times the Hush account was accessed. [PX 36; Tr. 159:22-161:12; 162:3:163:2.] For example, on April 23, at 10:14 PM PDT, the Mark Hopkins records show that Salyards' connected to the internet. [PX 36 at IHG0000005.] When analyzed together with the April 13 Hush Log, which shows a login from the Mark Hopkins at 10:15 PM PDT [App. B, No. 50], Salyards' exact sequence from accessing the internet from his hotel room to then logging in to the April 13 Email account is clear from the records.

Thereafter, on Monday April 27 at 1:26 PM CDT [App. B, No. 54], the first workday after Salyards left San Francisco (on Friday, April 24), the account was accessed from Salyards' Business IP. [PX 49.] Again, the likelihood that a spoofer would be able to accurately capture the different IP addresses corresponding so precisely to Salyards' moving whereabouts is not credible. Instead, the changes in the IP address captured by Hush sync with Salyards' stay at the hotel – both to and from San Francisco. Each time the April 13 Email account was accessed, it was done so from Salyards' exact geographical location.

It cannot be sheer coincidence that the April 13 Hush Log reflects two separate logins from the Mark Hopkins in San Francisco while Salyards was staying there. At the hearing,

Salyards sought to distract from the clear import of the Mark Hopkins records because his invoice specifically references an IP address ending ".12" while the Hush log reflects an address with the same first eight digits, but ending ".2" – even though both addresses indisputably are registered to the hotel. [Tr. 159:18-159:2.] However, that is a red-herring for various reasons: (1) As Obuchowski explained, the ".12" address is identified on the invoice only in relation to when Salyards – who paid for multiple rooms – purchased higher levels of internet service. No specific IP address is identified on the Mark Hopkins records when the lower-level basic service is purchased. For each time when the Hush account was accessed from the Mark Hopkins, Salyards had paid for a room in which basic service – without the ".12" address – was being used. [Tr. 186:1-13; 191:23-192:20; 195:24-196:8; 240:21-241:16.] (2) As Obuchowski further explained – based on dozens of criminal investigations as a member of his computer forensics task force – the ".2" address is one of many IP addresses indisputably owned by the Mark Hopkins and apparently used for outbound internet traffic (such as accessing the Hush website). [Tr. 191:8-22; 194:14-19; 613:3-614:20; 617:21-618:8.] (3) The ".2" address on the Hush log also could relate to usage of Salyards' laptop in hotel common areas or even that he accessed Hush from the hotel's business center. [Tr. 613:23-614:17.]

Even, however, if 2FA's argument about the operation of the Mark Hopkins IP addresses were accepted (despite its technical impossibility), then it actually would contradict any spoofing defense. If the only IP address used by Salyards at the Mark Hopkins was the ".12" IP address, there is no explanation how someone would have spoofed the ".2" IP address, which is the IP address that appears on the April 13 Hush Log.

2. Evidence Shows Collier Not the Author of April 13 Email:

Salyards presents deposition testimony from Chris Collier – a disgruntled former Passlogix employee – who now claims to have authored the April 13 Email. (Notably, he does

not know who wrote the September 3 Email.) It has come to light that Collier, even while an employee of Passlogix, had engaged in extensive unauthorized dealings with Salyards/2FA, which were kept secret from Passlogix. Indeed, before he testified at deposition, Collier and Salyards acknowledge discussing the substance of his testimony, while Collier contemporaneously was disavowing any knowledge of the emails to Passlogix and its lawyers. [Collier Tr. 121:3-124:22] According to Collier's testimony, he wrote the April 13 Email while working (unbeknownst to Passlogix) from 2FA's office, and based on information received from 2FA about a potential transaction with Wal-Mart. [Tr. 108:15-22.] In fact, the evidence conclusively demonstrates that Collier did not author the April 13 Email account:

a. Claimed IP Spoofing Not Possible: The computer program Collier claims to have used does not have the technical capabilities to alter an IP address assigned by an ISP, such as the IP addresses reflected in the Hush logs. Collier testified that he used the program "Mac IP Change" to conceal his own IP address and "spoof" Salyards' IP. [Collier Tr. 86:23-25.] However, Obuchowski explained the software program Mac IP Change, "does not have the technical capability of changing an IP address that's assigned by Time Warner to make it appear that you are coming from 2FA's network unless you were actually on 2FA's network. That program does not have that capability as Mr. Collier claims." [Tr. 164:7-11; PX 36 at ¶ 2-4] (emphasis added.) Nor do other computer programs. [Tr. at 242:12-16, 623:17-624:2.] Obuchowski also independently tested the capabilities of MAC IP Change by downloading the program. [Tr. 242:23-243:1.] Even after disclosure of Obuchowski's expert declaration stating that MAC IP Change did not have the technical capabilities to spoof an IP address as was done here, neither Salyards nor Cuttill (self-proclaimed IP spoofers) never adduced any contrary proof and never even tested the program. [Tr. 591:21-24.] Since the program that Collier claims to

have used to spoof does not have that technical capability (nor do other similar programs), then he could not have been the author of the April 13 Email.

b. Collier Testified Incorrectly About Basic Facts Concerning the April 13 Email Account: Collier repeatedly got basic facts wrong concerning the email account:

- He testified that he created the account "days before" he claims to have sent the email. [Collier Tr. 84:10-12, 85:20-86:1.] However, the April 13 Hush Log shows that the account was created the same day the email was sent, only 27 minutes before its transmission. [PX 49; App. B, No. 1.] This is significant not only because Collier got this basic fact wrong, but more importantly it undercuts any claimed "spoofing": had the account been set up "days before" – not at 2FA – then Collier's IP address (not Salyards') would have been captured by Hush.

- The April 13 Hush Log shows that the original April 13 Email was transmitted at 3:59 PM CDT [App. B, No. 16] and the account was then accessed twice more that afternoon – at 4:17 [App. B, No. 17] and 6:15 PM CDT [App. B, No. 18] – all from Salyards' Business IP. However, later that night, at 10:38 PM [App. B, No. 24], there was another login – this time from Salyards' Home IP, while the next day, on April 14, the account was again accessed from Salyards' Business IP [App. B, No. 30]. Those changes in the IP address usage contradict Collier's role. The record shows that there were no email communications between Salyards and Collier on April 13 and 14 at all – and Collier testified he simply copied 2FA email header properties and "did what anybody would do. . .just used the same IP" address each time. [Collier Tr. 88:10-12] (emphasis added.) He therefore would not have changed the "spoofed" IP addresses from Salyards' Business IP, to Salyards Home IP, and then back to Salyards' Business IP (in less than 24 hours), since Collier did not in the interim receive any new emails from Salyards, let alone emails reflecting different IP addresses.

- Collier testified to the password he used for the account (p-o0i9u8). [Collier Tr. at 85:8-15.] Even though the actual user successfully logged in ten times [PX 49], Collier was incorrect about the password. [PX 41; Tr. 166:2-25.]

- Collier testified that he was not even aware that Salyards was in San Francisco and that he and Salyards did not communicate by email during April. [Collier Tr. 63:19-22 and 126:16-127:4.] Accordingly, he could not have had access to any IP address – be it ".2" or ".12" from the Mark Hopkins hotel.[9]

- At the time the email was sent, Collier had only been a Passlogix employee for only twelve days [Tr. 48:25-49:1; 109:3-4]; yet, the author of the email claims to have worked on the Wal-Mart deal. [PX 2.] Collier never worked on the Wal-Mart deal. [Tr. 109:12-14.]

- The email references the author's unwillingness to continue working with "Sean Harris," but Collier testified that he had never even met Sean Harris. [Collier Tr. 111:19-21]. Collier testified that Cuttill was the source for the Sean Harris claim as well as all the other information contained in the email. [Collier Tr. 108:15-22.]

- The author of the April claims to "confirmed [the information] first-hand with two different sources." Collier however, could only name one person: Shaun Cuttill. [Collier Tr. 112:1-6.]

- Collier also testified that, while a Passlogix employee, he spoke to Salyards 15-20 times. [Collier Tr. 118:13-15] However, Collier's phone and email/text message records show that the he and Salyards had hundreds of communications during this period. [PX 45.]

---

[9] Salyards submitted an affidavit [PX 43 at ¶ 5e] conveniently asserting that emailed Collier from the Mark Hopkins, but Collier testified otherwise and Salyards has no copy of any purported email. Tellingly, Salyards produced – specifically for this hearing – six other emails that he sent while at the Mark Hopkins, but none were to Collier. [DX 7.]

c. Computer Records Rebut Collier's Testimony: Forensic evidence from Collier's work computer is inconsistent with Collier's claims to have sent the April 13 Email. Collier testified to sending the email from his personal computer while at 2FA's offices at 3:59 PM CDT, not his work computer. [Collier Tr. at 89:13-15] However, the evidence uncovered shows that his work computer was being actively used from 3:25 PM CDT to 4:55 PM CDT on April 13, by someone with the "user name chrisc and full name under that was Chris Collier." [Tr. 482:16-20.] Specifically, a network printer was being installed during this time, which required active user participation and the computer had to be connected to a network where the printer was located during the installation process – which it was – and that network was not 2FA's. [Tr. 492:5-13.] In addition to the printer installation, there also was a consistent level of internet and email activity from the computer that refutes he was elsewhere, using another computer. [Tr. 483:19-484:4] Because Collier could not have been in two different locations at the same time, and definitive (and unrebutted) computer forensic evidence show that he was using his work computer at a location other than 2FA at the time the email was transmitted, he could not have sent the April 13 Email.

d. Collier's/2FA's Account of April 13 Does Not Hold Up: Even if the unassailable forensic evidence was ignored (which of course it should not be), Collier's/2FA's accounts of the day's events leading to the 3:59 PM CDT transmittal of the April 13 Email do not hold up:

- According to Cuttill, Collier arrived at 2FA's offices that day around 3:00 PM CDT and that he greeted him at the door and then they went into his office to have a discussion that lasted approximately 10 minutes. [Tr. 594:9-21.] However, Collier's phone records show that he was on a phone call for 13 minutes between 3:02 and 3:15 PM CDT. [PX 45 at CC0010, Item 212.]
- At 3:32 PM CDT, the April 13 Email account at Hush was set up [App. B, No. 1], which is a process that takes time from beginning to end. [PX 49] However, at 3:27 PM CDT, Collier

sent an email from his Passlogix email account to another Passlogix employee – leaving virtually no time to have proceeded through the set-up process. [PX 56.]

- At 3:39 PM CDT, Collier began a 16 minute phone call with a Passlogix employee, ending at 3:55 PM CDT. [PX 45 at CC010, Item 213.] 2FA's version of the events leaves Collier only four minutes – his phone call ended at 3:55 PM CDT and the email was transmitted at 3:59 PM CDT [App. B, No. 16] – to compose the April 13 Email, which was full of information that Collier claimed he did not independently know but learned from Cuttill. [Collier Tr. 108:15-110:15.] This story is simply not credible.

- But it does not end with the email's transmission. The April 13 Hush Log shows that the account was accessed twice later that afternoon – at 4:17 PM [App. B, No. 17] and then again at 6:15 PM [App. B, No. 18], both CDT. Yet, during this time period, Cuttill testified that he was meeting with Collier in 2FA's conference room. [Tr. 595:6-23.]

e. Collier Lacks Credibility as a Witness: Collier is clearly not a credible witness for multiple reasons. During Passlogix's internal investigation and, prior to his deposition, Collier repeatedly disclaimed any knowledge of the emails to Passlogix. [Collier Tr. 126:1-2.] Collier now claims that he was not then telling the truth; he claims that before his deposition, he disclosed to Salyards what he knew while simultaneously concealing the information during discussions with Passlogix until his deposition testimony. [Collier Tr. 121:3-124:3.] There was friction between Passlogix and Collier, who had a severance dispute when he left Passlogix during an initial tenure, and then only came back in April 2009 for less than eight months as part of a larger group from the company whose assets Imprivata acquired. [Tr. 36:25-37:4; 43:22-25.] Collier also testified to (and Salyards' corroborated) extensive, secret communications with Salyards throughout his tenure at Passlogix. Aside from the extensive phone calls, text messages and Skype messages and office visits (which no longer exist because Salyards destroyed them),

Collier testified to conducting secret "Passlogix" business with 2FA from his personal email account so that no one from Passlogix would catch him communicating with 2FA. [Collier Tr. 116:12-118:12.] He also testified that 2FA was the only instance that he used his personal email account to conduct Passlogix business. [Collier Tr. 120:1-5.] This was all done without the knowledge of Passlogix management, including Collier's direct supervisor. [Tr. 108:13-109:2][10]

III. OTHER ASPECTS OF THE RECORD CORROBORATE SALYARDS' CULPABILITY

Standing on its own, the computer forensic evidence speaks for itself in unequivocally identifying Salyards as the source of the emails. Nowhere does Salyards offer any credible explanation to counter that hard evidence. Without distracting from the gravity of the internet records, additional miscellaneous evidence only further corroborates Salyards' culpability:

First, Salyards failed to present available records or even take basic steps to recover data that would corroborate his position. Specifically, he offered no data showing that Collier accessed the 2FA network on April 13; no data showing that his own computers were not in use on April 13 or September 3 at the relevant times; and no data showing that he was not using the internet at the Mark Hopkins during the relevant times. Even though Salyards and Cuttill testified to conducting computer forensic investigations in the past, they made no serious effort here. The absence of supporting documentation belies his position. To the extent Salyards contends such data does not exist, basic steps are available to recover such data, such as seeking assistance from a third-party recovery service to recover computer/network records or information from April 13 or September 3. Indeed, Salyards has taken advantage of such data

[10] Notably, Collier told the internal investigation that Passlogix made "very clear we are not to disclose the proprietary information from a previous employer" [PX 35 at PL0095990] and maintained at his deposition he was aware of no intellectual property misuse by anyone at Passlogix. [Collier Tr. 97:2-16.]

recovery services before. In 2008, when Salyards' computer crashed, he sent his computer to a data recovery service (and 2FA produced 50 pages worth of documentation to confirm this). Here, however – in the face of these allegations, 2FA made no demonstrable effort whatsoever to recover anything.

Second, there is a striking similarity of key phrases appearing in both emails at issue and other Salyards' writings:

- By email dated September 29, 2006, Salyards wrote Passlogix executives to complain that they had "treated us like second class citizens." [PX 9 at PL0016517.] Likewise, the author of the September 3 Email uses the same language: "I have been treated like a second-class citizen." [PX 1.]

- As shown to the linguist Perlman, both the September 3 and April 13 Emails use language that otherwise is notable in Salyards' writings. By way of just a few examples: compare PX 1 (using "organisation" four times)[11] with PX 6 (using "organization" six times); compare PX 1 (offering an "apology" to recipient) with PX 6 at PL0042567-68 (offering twice an "apology"/"apologize" to recipient), PX 12 at PL0031385 ("apology" to recipient) and PX 13 at PL0031594 ("apologize" to recipient); compare PX 1 ("Upon my transition . . .") with PX 6 at PL0042567 ("Upon my arrival . . .") and PX 7 at PL0042559 ("Upon discussing . . ."); compare PX 1 (refers to "Hey guys" and "guys") with PX 9 at PL0016517 ("hey guys") and PX 10 at PL0016524-25 (refers to "guys" three times); compare PX 2 ("Honestly, . . .") with PX 10 at PL0016524 ("honestly" twice) and PX 13 at PL0031594 ("To be honest . . .,").

[11] Although the September 3 Email uses the U.K.-practice for spelling "organization" with an "s", that is a well-known style easily adopted to disguise authorship; in fact, other words in the September 3 Email tellingly do not display the U.K. characteristic spelling. [Tr. 295:18-296:2.]

- When Passlogix's CEO Boroditsky received the April 13 Email, he promptly replied to the sender that it sounded like someone with "an axe to grind." [PX 26.] Salyards states he did not see Boroditsky's April 13 response until well after September 3, since he claims not to have been involved in the activity associated with the April 13 Email. [Tr. 339:14-340:25.] After the September 3 Email was sent, however, Salyards replied by repeating the same phrase from Boroditsky's response to the April 13 Email: "it appears as if one of your employees has an axe to grind." [PX 29.]

Third, Salyards' conduct is, to say the least, extremely suspicious immediately following Passlogix's letter to the Court about the emails, sent to 2FA's counsel on October 27, 2009 at 4:30 PM CDT. [PX 33.] Less than one hour later, at 5:56 PM CDT, Salyards sent a Skype instant message to Collier, saying "call me." [PX 50 at PL009618016 (Page 249).] Seven minutes later, at 5:53 CDT, Collier called Salyards and they spoke for six minutes. [PX 45 at CC0124.] Less than an hour later, at 6:44 PM CDT, Salyards sent Collier a text message. [PX 45 at CC0128.] Later that night, at 12:25 AM CDT, Salyards sent Collier another text message. [PX 45 at CC0141.] The first thing the next morning, at 8:19 AM CDT, Collier called Salyards and they spoke for twelve minutes. [PX 45 at CC0136] This was by far the earliest the two had ever spoken before. Then, between 9:18 AM CDT and 9:47 AM CDT, Collier and Salyards exchanged five text messages. Later that afternoon, at 2:24, Collier and Cuttill spoke on the phone for six minutes.

Given what Salyards had just been accused of, the only plausible reason that he was so urgently speaking with Collier was that Salyards was involved and was taking steps to fabricate his defense. It makes no sense why – if Salyards had no role – he would have spoken to Collier ten times during this critical 16-hour period (which includes the overnight) immediately after Passlogix wrote to the Court.

IV. UNDER CONTROLLING LAW, SALYARDS' FRAUDULENT MISCONDUCT AS EMAIL SOURCE WARRANTS SEVERE SANCTIONS

By his actions, Salyards persistently sought to exploit the September 3 Email to pervert the judicial process: immediately after its transmittal, he took advantage of it for settlement leverage and to seek more expansive discovery into, among other things, a highly confidential Passlogix project under development. Under oath, Salyards repeatedly has stated he did not play a role in the transmittal of the September 3 or April 13 Emails. Yet, it is literally uncontroverted – and dispositive – that objective computer logs identify the source of the relevant email activity as Salyards' two regular IP addresses and the San Francisco hotel IP address where he was staying for the applicable period. The expert analysis of Obuchowki also stands unrebutted on the point that any claimed IP spoofing is infeasible and cannot apply here. To support his testimony, Salyards – who aggressively pursued discovery from Passlogix on these matters – offers no expert to address the technical proof, offers no competent evidence on an alternative source for the critical September 13 Email, and relies merely on the flawed and suspect testimony of Collier for the April 13 Email and alleged records that he since has destroyed.

If, as the overwhelmingly lopsided evidence has borne out, Salyards is culpable for the deceptive September 3 Email, he has committed a serious fraud on the Court – he has misused the email to try to manipulate events in the case, and he then has testified falsely about it on repeated occasions. Rigorous sanctions for such fraudulent misconduct are appropriate where, as here, it is "established by clear and convincing evidence that a party has 'sentiently set in motion some unconscionable scheme calculated to interfere with the judicial system's ability impartially to adjudicate a matter.'" Hargrove v. Riley, No. 04 Civ. 4587, U.S. Dist. LEXIS 6899 at *11 (E.D.N.Y. Jan. 31, 2007) (quoting McMunn v. Mem'l Sloan-Kettering Cancer Ctr., 191 F. Supp. 2d 440, 445 (S.D.N.Y. 2002)); see also Shangold v. The Walt Disney Co., No. 03 Civ. 9522,

2006 WL 71672, at *1, *3 (S.D.N.Y. Jan, 12, 2006) (finding clear and convincing evidence of fraud where plaintiffs fabricated a timeline and plot outlines to advance their claims); Scholastic, Inc. v. Stouffer, 221 F. Supp. 2d 425, 444 (S.D.N.Y. 2002) (imposing sanctions where Court found "by clear and convincing evidence that [party] has perpetrated a fraud on the Court through submission of fraudulent documents as well as through her untruthful testimony"); McMunn, 191 F. Supp. 2d at 446 (finding clear and convincing evidence of fraud where plaintiff edited audio tapes and represented that they were unedited during discovery).

Given the gravity of the misconduct, dismissal of Salyards/2FA's pleading is a proper sanction: "[w]hen a party lies to the court and his adversary intentionally, repeatedly," its pleading should be dismissed Shangold, 2006 WL 71672 at *4 (dismissing where plaintiffs fabricated evidence to advance their claims, and refused to "relent . . . [e]ven . . . in the face of indisputable evidence" of the fabrication); see also Hargrove, 2007 U.S. Dist. LEXIS 6899 at *38 (dismissing where plaintiff submitted multiple forgeries to defendants and the court, "never corrected them once their authenticity was challenged and [] continue[d] to insist on their veracity"); McMunn, 191 F. Supp. 2d at 445 (dismissal where plaintiff "lie[d] to the court and his adversary intentionally, repeatedly" by falsifying deposition testimony, editing certain tapes, among other things); Cerutti 1881 S.A. v. Ceruti, Inc., 169 F.R.D. 573, 583 (S.D.N.Y. 1996) (entering judgment for plaintiff where defendants submitted fraudulent documents, gave false deposition testimony, and "did not withdraw the [fraudulent] documents on their own," but "[r]ather . . . waited until the falsity of the documents had been detected"). In such a case, "it can fairly be said that [the offender] has forfeited his right to have his claim decided on the merits." Shangold, 2006 WL 71672 at *4.

In addition to the dismissal of his pleading, Salyards also as a sanction should be required to reimburse Passlogix for its costs attendant to investigating and addressing the serious issues of

the falsified emails. Monetary sanctions also are proper where, as here, a party has fabricated evidence. Shangold, 2006 WL 71672 at *5 ("For more than two years, Plaintiffs have imposed substantial burdens on Defendants including attorneys' fees, costs and the attendant inconvenience and distraction of defending this litigation. Accordingly, . . . an award of attorneys' fees and costs is appropriate . . ."); Scholastic, 221 F. Supp. 2d at 444 (monetary sanctions against party that fabricated evidence were "appropriate given the fact that Stouffer has engaged in a pattern of intentional bad faith conduct and failed to correct her fraudulent submissions, even when confronted with evidence undermining the validity of those submissions"); McMunn, 191 F. Supp. 2d at 462 (imposing "a monetary sanction that represents the additional costs, fees, and expenses incurred by Memorial due to Ms. McMunn's misbehavior"); Cerutti, 169 F.R.D. at 584 ("It is also proper. . .to assess costs and attorneys' fees, because defendants' conduct led plaintiffs' counsel on an arduous chase").

Here, the costs for which Passlogix is entitled to reimbursement are substantial. Passlogix turned its company upside down in the immediate aftermath of the September 3 Email, incurring in excess of $50,000 for outside counsel fees to interview over 25 employees about the underlying allegations. Thereafter, it spent much more than that in its dealings with non-party Imprivata and on developing the record about the emails. To that end, it was forced to pursue formal discovery in Canada from Hush, retain experts to assist in analyzing the pertinent computer/email data, respond to the expansive discovery demands propounded by Salyards in connection with these matters, and compile and present the evidence it adduced at the hearing. Upon a judicial finding of culpability on Salyards' part for the subject emails, Passlogix will be prepared to quantify the full costs for reimbursement approval by the Court.

V. SALYARDS/2FA ENGAGED IN SPOLIATION OF CORE INFORMATION, WHICH INDEPENDENTLY JUSTIFIES SEVERE SANCTIONS

As an independent basis for sanctions, Salyards' admits to the destruction of basic records relating to the relevant email activity. Indeed, Salyards states that no document preservation policy was implemented during the pendency of the litigation – which, standing by itself, is a significant breach of a party's fundamental obligations.[12] See Pension Cmm. of Univ. of Montreal Pension Plan v. Banc of Am. Secs., LLC, No. 05 Civ. 9016, 2010 WL 184312 at *4 (S.D.N.Y., Jan. 15, 2010) (party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents"). The destruction of evidence on Salyards' part includes;

- Salyards claims that, in June or July 2009, he received an anonymous email from another Hush account that attached Passlogix technical specifications very similar to the September 3 Email attachment. He claims to have spent upwards to an hour reviewing the June/July attachment, and also showed it to Cuttill for review. Without producing or even disclosing the email to anyone at Passlogix, Salyards claims to have deleted it – and remained silent even though it clearly is responsive to discovery in the case, and even after it was known that Passlogix was spending resources investigating the anonymous September 3 Email from Hush. [Tr. 356:1-359:1.] He only referenced the alleged June/July email at his deposition on October 23, and by then – despite his claimed technical expertise – the email allegedly no longer was recoverable.

- Salyards states that he and Collier, while Collier was employed by Passlogix from April 1 through November 16, 2009, engaged in extensive communications that were kept secret from Passlogix and utilized Collier's private email account outside of Passlogix. Even according to Salyards' own count for the less than eight month period, they communicated by text messaging over 91 times [PX 47 at 11888], by Skype messaging roughly 40 times, and by email roughly 12 times – but he deleted each one of those over

---

[12] A litigant "is under a duty to preserve what it knows, or reasonably should know, is relevant in the action" Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72-73 (S.D.N.Y. 1991) (defendant was on notice "at least by the time the complaint was served" that it should have preserved evidence that was subsequently destroyed); Chan v. Triple 8 Palace, Inc. No. 08 Civ. 6048, 2005 WL 1925579, at *10 (S.D.N.Y. Aug. 11, 2005) (sanctions appropriate where party "permitted the ongoing destruction of material evidence after litigation had been initiated"); see also In re NTL, Inc. Secs. Litig., 244 F.R.D. 179, 193 (S.D.N.Y. 2007) (quoting Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998)) (a party's obligation to preserve arises "when a party should have known that the evidence may be relevant to future litigation").

150 written communications. Even though Salyards relies heavily on Collier, none of these communications with his key corroborator apparently are recoverable. (The two also spoke by phone over 81 times). [PX 47 at 11881.]

- For the first time at the hearing, Cuttill disclosed that he reviewed 2FA network and computer logs. [Tr. 573-576.] Even though he did so, not a single 2FA computer or network log was produced because the logs were not helpful to 2FA. [Tr. 575:8-12.] Cuttill also specifically reviewed Salyards' computer logs, but chose not to produce the Salyards' logs "because the logs were tainted" [Tr. 577:1]; "inconclusive" [Tr. 575:25; 578: 8, 14, 24]; and in Cuttill's own words, only produced information that would assist it in exonerating Salyards, but not anything else. [Tr. 576:6-581:1.]

Notwithstanding the fact that Passlogix made comprehensive disclosures (including its internal investigation documents) concerning the emails, 2FA consistently obstructed timely, orderly disclosures relating to information about the emails it possessed. Cuttill was asked at his deposition about any steps taken to investigate the source of the email activity. His lawyer blocked the testimony on grounds of attorney client privilege and work product. Yet, the lawyer later advised the Magistrate Judge that counsel was not involved in any investigation.[13] [12/22 Tr. 26:12-16.] At the hearing, Cuttill acknowledged that he and Salyards knew, by the time of the Cuttill deposition, the substance of Collier's testimony that he later would provide at his deposition, but concealed it from Passlogix by invoking privilege – even though it was purely factual matter, and counsel concededly was not involved. [Tr. 596:22-597:9.] This is a classic example of litigation by ambush; it is improper. Relatedly, Cuttill testified to speaking with other 2FA employees/staff and researching various internet matters connected with the emails – yet, no notes or any other memorialization of any investigation was produced to test the veracity of his self-serving statements.[14]

---

[13] 2FA's "informal investigation" – conducted without counsel, during which no notes were taken or documents collected – pales in comparison to the extensive and costly efforts undertaken by Passlogix to get to the bottom of these issues.

[14] For example, for the first time at the hearing, Cuttill stated –without furnishing any data – that he allegedly clocked the time it takes to start up a computer and login to an account. [Tr. 562:6-

Two separate legal consequences arise from 2FA's clear-cut disclosure failures:

First, an adverse inference should be drawn and Salyards precluded from making arguments that implicate the very documents he discarded. "The spoliation of evidence germane 'to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction.'" Byrnie v. Town of Cromwell Board of Educ., 243 F.3d 93, 107 (2d Cir. 2001) (quoting Kronisch v United States, 150 F.3d 112, 126 (2d Cir. 1998) (adverse inference is warranted where defendant was obligated to preserve certain documents that were relevant to plaintiff's case, but intentionally destroyed them); Brown v. Coleman, No. 07 Civ. 1345, 2009 WL 2877602 (S.D.N.Y. Sept. 8, 2009). Indeed, an adverse inference arises through a showing "that the evidence was destroyed 'knowingly, even if without intent to [breach a duty to preserve it], or *negligently*.'" Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (quoting Byrnie, 243 F.3d at 109) (emphasis in original).

Here, Salyards should be precluded from arguing that Collier somehow traced Salyards' whereabouts by email and somehow spoofed Salyards' changing IP addresses from office, to home, to the San Francisco hotel. In fact, Collier testified he did not email with Salyards in April when Salyards was in San Francisco – and therefore would not have been able to spoof the San Francisco IP address. Only Salyards by way of a self serving affidavit states he sent an email from San Francisco on April 19 to Collier. But given Collier's testimony that he did not then email with Salyards, and Salyards' inability to produce any claimed email, he should not be permitted to make the argument based on allegedly deleted email communications with Collier at

---

564:8.] In contrast, Passlogix appropriately relied on expert testimony based on written findings disclosed before the hearing. [PX 36, 44, 55.]

the time. In the absence of such email activity, it becomes impossible for Collier even under Salyards' theory to have spoofed the San Francisco IP address.

Second, Salyards should be responsible for Passlogix's costs because his destruction of emails and other records caused Passlogix's investigation to be far more costly and protracted. It is proper to "impose monetary sanctions for the destruction of evidence." Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 77 (S.D.N.Y. 1991) ("an award of costs, including attorneys' fees, is entirely warranted" where defendant "unjustifiably destroyed documents after litigation had been commenced, causing the plaintiff to expend time and effort in attempting to track down the relevant information"). "Such compensable costs may arise either from the discovery necessary to identify alternative sources of information, or from the investigation and litigation of the document destruction itself." Id. at 78. If Salyards had preserved the claimed June/July email form Hush and attachment (assuming it occurred), and preserved his extensive written communications with Collier (even to any meaningful degree), the ability to ascertain the comprehensive facts – and test the bona fides of Salyards' assertions – would have been far more efficient. Instead, Salyards' broad-brush discarding of information substantially increased the burden and expense for Passlogix to compile the forensic and other evidence concerning both relevant Hush-related email activity, and Salyards and Collier's contentions about where and how they accessed the internet at relevant times.

CONCLUSION

Accordingly, Passlogix has demonstrated, by clear and convincing evidence, that Salyards is the source of the emails at issue, testified falsely under oath about his role, and spoliated core relevant information. Passlogix respectfully submits that rigorous sanctions are warranted, consisting of dismissal of Salyards/2FA's pleading and the imposition of costs for Passlogix's investigation into the origin and circumstances of the emails.

Dated: February 1, 2010

PROSKAUER ROSE LLP

By: Hal S. Shaftel

Hal. S. Shaftel (HS-0627)
Daniel P. Goldberger (DG-2440)
Proskauer Rose LLP
1585 Broadway
New York, NY 10036
Tel. (212) 969-3000
Fax (212) 969-2900

Attorneys for Plaintiff Passlogix, Inc.

APPENDIX A

APPENDIX A
SEPTEMBER 3 HUSH LOG

	Log entry report for: passlogix-vgo-saw@hushmail.me		
Number	**date**	**SALYARDS' TIME**	**command**
1	9/3/2009 19:10	2:10 PM CDT	New account (4) success
2	9/3/2009 19:10	2:10 PM CDT	New account (4) creating account without java
3	9/3/2009 19:10	2:10 PM CDT	Account created in non-Java mode
4	9/3/2009 19:14	2:14 PM CDT	login_attempt
5	9/3/2009 19:14	2:14 PM CDT	Login completed without Java
6	9/3/2009 19:14	2:14 PM CDT	login_success
7	9/3/2009 19:14	2:14 PM CDT	no contacts message to migrate
8	9/3/2009 19:14	2:14 PM CDT	Opened folder: INBOX (1 messages)
9	9/3/2009 20:57	3:57 PM CDT	Encryption not available for marcb@passlogix.com
10	9/3/2009 20:57	3:57 PM CDT	Checking if encryption method is available for: passlogix-vgo-saw@hus
11	9/3/2009 21:00	4:00 PM CDT	Sending message to 6 recipient(s) - message id dfeda8871a9740fe
12	9/3/2009 21:00	4:00 PM CDT	outgoing message
13	9/3/2009 21:00	4:00 PM CDT	abuse_check - sending to enough recipients to be checked (6)
14	9/3/2009 21:00	4:00 PM CDT	abuse_check - sending to enough recipients to be checked (6)
15	9/3/2009 21:00	4:00 PM CDT	Message sent from 'passlogix-vgo-saw@hushmail.me' to: marcb@pass
16	9/3/2009 21:49	4:49 PM CDT	Opened folder: INBOX (3 messages)
17	9/3/2009 21:49	4:49 PM CDT	Reading message as text
18	9/3/2009 21:49	4:49 PM CDT	read message: Folder: INBOX
19	9/3/2009 21:49	4:49 PM CDT	Reading message as text
20	9/3/2009 21:49	4:49 PM CDT	read message: Folder: INBOX
21	9/3/2009 21:50	4:50 PM CDT	Opened folder: INBOX (3 messages)
22	9/4/2009 0:16	7:16 PM CDT on 9/3	login_attempt
23	9/4/2009 0:16	7:16 PM CDT on 9/3	Login completed without Java
24	9/4/2009 0:16	7:16 PM CDT on 9/3	login_success
25	9/4/2009 0:16	7:16 PM CDT on 9/3	Opened folder: INBOX (4 messages)
26	9/4/2009 19:22	2:22 PM CDT	login_attempt
27	9/4/2009 19:22	2:22 PM CDT	Login completed without Java
28	9/4/2009 19:22	2:22 PM CDT	login_success
29	9/4/2009 19:22	2:22 PM CDT	Opened folder: INBOX (4 messages)

APPENDIX B

APPENDIX B
APRIL 13 HUSH LOG

	Log entry report for: concernedatpasslogix@hushmail.com			
Number	Date	SALYARDS' TIME	Command	IP
1	4/13/2009 20:32	3:32 PM CDT	New account(3) new_account_token match: 49e3a14c15922	70.114.246.62
2	4/13/2009 20:32	3:32 PM CDT	New account (3) turing success: concernedatpasslogix@hushmail.com	70.114.246.62
3	4/13/2009 20:32	3:32 PM CDT	New account (3) creating account without java: concernedatpasslogix@hushmail.com	70.114.246.62
4	4/13/2009 20:32	3:32 PM CDT	New account (3) success: concernedatpasslogix@hushmail.com	70.114.246.62
5	4/13/2009 20:32	3:32 PM CDT	New account (3) turing code age: 198	70.114.246.62
6	4/13/2009 20:32	3:32 PM CDT	login_attempt	70.114.246.62
7	4/13/2009 20:32	3:32 PM CDT	no contacts message to migrate	70.114.246.62
8	4/13/2009 20:32	3:32 PM CDT	login_success	70.114.246.62
9	4/13/2009 20:32	3:32 PM CDT	Login completed without Java	70.114.246.62
10	4/13/2009 20:32	3:32 PM CDT	Opened folder: INBOX (1 messages)	70.114.246.62
11	4/13/2009 20:33	3:33 PM CDT	Time to retrieve pseudonyms: 0.089392185211182 seconds	70.114.246.62
12	4/13/2009 20:58	3:58 PM CDT	Checking if encryption method is available for: marcb@passlogix.com	70.114.246.62
13	4/13/2009 20:58	3:58 PM CDT	Encryption not available for marcb@passlogix.com	70.114.246.62
14	4/13/2009 20:59	3:59 PM CDT	outgoing message	70.114.246.62
15	4/13/2009 20:59	3:59 PM CDT	Sending message to 2 recipient(s) - message id 0dc89735a3c8df3a	70.114.246.62
16	4/13/2009 20:59	3:59 PM CDT	Message sent from 'concernedatpasslogix@hushmail.com' to: marcb@passlogix.com	70.114.246.62
17	4/13/2009 21:17	4:17 PM CDT	Opened folder: INBOX (1 messages)	70.114.246.62
18	4/13/2009 23:15	6:15 PM CDT	login_attempt	70.114.246.62
19	4/13/2009 23:15	6:15 PM CDT	login_success	70.114.246.62
20	4/13/2009 23:15	6:15 PM CDT	Login completed without Java	70.114.246.62
21	4/13/2009 23:15	6:15 PM CDT	Opened folder: INBOX (2 messages)	70.114.246.62
22	4/13/2009 23:15	6:15 PM CDT	read message: Folder: INBOX	70.114.246.62
23	4/13/2009 23:15	6:15 PM CDT	Reading message as text	70.114.246.62
24	4/14/2009 3:38	10:38 PM CDT 4/13	login_attempt	70.114.204.202
25	4/14/2009 3:39	10:39 PM CDT 4/13	login_success	70.114.204.202
26	4/14/2009 3:39	10:39 PM CDT 4/13	Login completed without Java	70.114.204.202
27	4/14/2009 3:39	10:39 PM CDT 4/13	Opened folder: INBOX (2 messages)	70.114.204.202
28	4/14/2009 3:39	10:39 PM CDT 4/13	read message: Folder: INBOX	70.114.204.202
29	4/14/2009 3:39	10:39 PM CDT 4/13	Reading message as text	70.114.204.202
30	4/14/2009 20:19	3:19 PM CDT	login_attempt	70.114.246.62
31	4/14/2009 20:19	3:19 PM CDT	login_success	70.114.246.62
32	4/14/2009 20:19	3:19 PM CDT	Login completed without Java	70.114.246.62
33	4/14/2009 20:19	3:19 PM CDT	Opened folder: INBOX (2 messages)	70.114.246.62
34	4/16/2009 1:58	8:58 PM CDT 4/15	login_attempt	70.114.246.62
35	4/16/2009 1:59	8:59 PM CDT 4/15	login_success	70.114.246.62
36	4/16/2009 1:59	8:59 PM CDT 4/15	Login completed without Java	70.114.246.62
37	4/16/2009 1:59	8:59 PM CDT 4/15	Opened folder: INBOX (2 messages)	70.114.246.62
38	4/16/2009 15:29	10:29 AM CDT	login_attempt	70.114.246.62
39	4/16/2009 15:29	10:29 AM CDT	login_success	70.114.246.62
40	4/16/2009 15:29	10:29 AM CDT	Login completed without Java	70.114.246.62
41	4/16/2009 15:29	10:29 AM CDT	Opened folder: INBOX (2 messages)	70.114.246.62
42	4/17/2009 15:31	10:31 AM CDT	login_attempt	70.114.246.62
43	4/17/2009 15:31	10:31 AM CDT	login_success	70.114.246.62
44	4/17/2009 15:31	10:31 AM CDT	Login completed without Java	70.114.246.62
45	4/17/2009 15:31	10:31 AM CDT	Opened folder: INBOX (2 messages)	70.114.246.62
46	4/20/2009 17:30	10:30 AM PDT	login_attempt	64.186.161.2
47	4/20/2009 17:30	10:30 AM PDT	login_success	64.186.161.2
48	4/20/2009 17:30	10:30 AM PDT	Login completed wilhout Java	64.186.161.2
49	4/20/2009 17:30	10:30 AM PDT	Opened folder: INBOX (2 messages)	64.186.161.2
50	4/24/2009 5:15	10:15 PM PDT 4/23	login_attempt	64.186.161.2
51	4/24/2009 5:16	10:16 PM PDT 4/23	login_success	64.186.161.2
52	4/24/2009 5:16	10:16 PM PDT 4/23	Login completed wilhout Java	64.186.161.2
53	4/24/2009 5:16	10:16 PM PDT 4/23	Opened folder: INBOX (2 messages)	64.186.161.2
54	4/27/2009 18:26	1:26 PM CDT	login_attempt	70.114.246.62
55	4/27/2009 18:26	1:26 PM CDT	login_success	70.114.246.62
56	4/27/2009 18:26	1:26 PM CDT	Login completed wilhout Java	70.114.246.62
57	4/27/2009 18:26	1:26 PM CDT	Opened folder: INBOX (2 messages)	70.114.246.62